REMARKS

Claims 1-20, 23-51 are pending, with claims 1, 9, 13, 30, 38, 42 and 50 being independent. Claims 1-49 were rejected in the office action mailed March 22, 2006. Claims 1-2, 5-7, 9, 11-17, 19, 23-24, 26-28, 30-31, 34-36, 38, 41-43, 45-46, and 48 are currently amended. Claims 21-22 are canceled. Claims 50-51 are new. No new matter is added. Reconsideration of the action is requested in light of the foregoing amendments and the following remarks.

Section 103 Rejection

Claims 1-7, 9-10, 12-17, 19, 23-28, 30-36, 38-39, 41-46, and 48 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Bruce Schneier, Applied Cryptography, second ed., 1996 ("Schneier"), in view of William Stallings, Cryptography and Network Security, second ed., 1998 ("Stallings").

Claim 1, as amended, recites in part a computer program product including instructions for a first application. A first container object is generated by the first application. The first container object includes a sender's certificate or a request for a recipient's certificate. The first container object is transmitted to a recipient using a second application distinct from the first application. The first application obtains a second container object from the second application. The first application automatically identifies and extracts one or more certificates from within the second container object.

Schneier discloses privacy-enhanced messages. *See* p. 579. The privacy enhanced messages are encrypted e-mail messages that include one or more certificates embedded within the body of the e-mail. *See id*; figs. 24.5 and 24.6. Schneier does not disclose or suggest automatically identifying and extracting one or more certificates. However, the examiner states that Stallings discloses automatically identifying and extracting certificates at fig. 14.6.

Stallings discloses a secure socket layer ("SSL") handshake protocol for establishing a logical connection between two computers. *See* p. 450. The SSL handshake protocol includes an exchange of several messages between a client and server in order to establish secure data transmission. *See* p. 450. The exchanged data includes hello messages, certificate messages, key exchange messages, verification messages, and certificate request messages. *See* p. 451, fig.

14.6. The examiner identifies the extraction of certificates from these messages as disclosing automatically identifying and extracting one or more certificates.

Stallings, however, teaches only that an SSL "client" performs the steps of transmitting and receiving messages. *See* p. 450, referring to "the client," emphasis added. *See also, e.g.,* http://www.openssl.org/support/faq.html, referring to "the OpenSSL library," emphasis added. At best, Stallings discloses that an SSL client or library identifies and extracts one or more certificates from the messages, and that this same SSL client or library transmits and receives messages as well. In contrast, claim 1 recites two distinct applications to perform the receiving and identifying operations. The recited first application automatically identifies and extracts certificates from a container object while the second application transmits and receives container objects. Stallings does not disclose or suggest receiving a container object using a first application and identifying and extracting a certificate using a second application.

The applicant respectfully submits that claim 1 and independent claims 9, 13, 23, 30, 38, 42, and 50, which contain similar limitations as claim 1, are condition for allowance. Claims 2-8, 10-12, 14-20, 24-29, 31-37, 39-41, 43-49, and 51 depend from these independent claims and are therefore also in condition for allowance.

Claim 5 depends from claim 1 and further recites that the computer program product includes instructions for determining whether the sender has multiple certificates. Neither Schneier nor Stallings discloses or suggests determining whether the sender has multiple certificates.

The applicant submits that the relied upon portions of Schneier do not disclose that a sender can have more than one certificate. The examiner relies on fig. 24.5, which discloses a single originator certificate, not a multiplicity of originator certificates. (The other certificate in fig. 24.5 does not belong to the sender; it belongs to the certificate authority which signed the sender's originator certificate. *See* p. 581.) Therefore Schneier does not disclose a sender having multiple certificates.

Furthermore, even assuming for the sake of argument that Schneier does disclose a sender having multiple certificate, Schneier does not disclose or suggest determining whether the sender has multiple certificates, as required by claim 5. Schneier merely discloses the format of the messages created. *See* fig. 24.5 and especially the heading for the relied upon portions, "PEM

Messages," and the opening sentence, "PEM's heart is its message format." Schneier does not disclose any kind of user interface for creating these messages, or any program at all which might determine whether the sender has multiple certificates. The reference simply assumes that a certificate has been chosen and used to encrypt a message.

Stallings does not remedy the deficiency of Schneier. The relied upon portions of Stallings do not teach that a sender can have multiple certificates. Indeed, the examiner does not purport to find this limitation in Stallings.

The applicant respectfully submits that claim 5, as well as claims 16, 26, and 34, which contain similar limitations, are in condition for allowance.

New Claims

Claims 50-51 are new. Claim 50 is an independent system claim reciting first and second instances of first and second applications. Claim 50 has features similar to those recited in claims 30, 38, 41, and 42, and is allowable for at least the same reasons. Claim 51 depends from claim 50 and is also allowable.

Conclusion

The applicant respectfully requests that all pending claims be allowed.

By responding in the foregoing remarks only to particular positions taken by the examiner, the applicant does not acquiesce with other positions that have not been explicitly addressed. In addition, the applicant's arguments for the patentability of a claim should not be understood as implying that no other reasons for the patentability of that claim exist.

Please apply any charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 14 July 2006

Brian J. Gustafson
Reg. No. 52,978

Customer No. 21876
Fish & Richardson P.C.
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

50338999.doc